IN THE UNITED STATES DISTICT COURT
FOR THE WESTERN DISTICT OF PENNSYLVANIA

BLAKE BOJE, individually and on behalf of all others similarly situated, **Plaintiff,**	)	**C.A. No. 23-46 Erie**
v.	)	**District Judge Susan Paradise Baxter**
MERCYHURST UNIVERSITY, Defendant.	)	

MEMORANDUM OPINION

I. INTRODUCTION

A. Relevant Procedural History

This action arises out of a 2022 data breach of the computer network at Mercyhurst University ("Mercyhurst"). On January 10, 2023, Plaintiff Blake Boje, a former Mercyhurst student, initiated this matter in the Court of Common Pleas of Erie County, Pennsylvania, by filing a complaint against Mercyhurst, both individually and on behalf of all individuals whose personal information was compromised in the breach. [ECF No. 1-2]. Mercyhurst subsequently removed the action to this Court by Notice of Removal filed on March 2, 2023. [ECF No. 1]

In general, Plaintiff alleges that Mercyhurst failed to properly secure and safeguard personally identifiable information ("PII") of its employees and students stored within its computer network, failed to provide adequate notification of the breach, and "obfuscate[ed] the nature of the breach." (ECF No. 1-2, at ¶ 9). The complaint sets forth six causes of action under state law: (1) negligence; (2) negligence per se; (3) breach of confidence; (4) breach of implied contract; (5) unjust enrichment; and (6) publicity given to private life.

On July 7, 2023, Mercyhurst filed a motion to dismiss Plaintiff's complaint for lack of subject matter jurisdiction, pursuant to Fed.R.Civ.P. 12(b)(1), and, alternatively, for failure to state a claim upon which relief may be granted, pursuant to Fed.R.Civ.P. 12(b)(6). [ECF No. 14]. Plaintiff has since filed a brief in opposition to Mercyhurst's motion [ECF No. 19], and Mercyhurst has filed a reply brief [ECF No. 20]. This matter is now ripe for consideration.

B. Relevant Factual History[1]

Plaintiff was a student at Mercyhurst from 2011-2015 (ECF No. 1-2, at ¶ 11). At some point between January 16 and May 15, 2022, a data breach of Mercyhurst's computer system occurred, during which cybercriminals gained unauthorized access to highly sensitive PII of Mercyhurst's current and former employees and students (the "Data Breach"). (Id. at ¶¶ 1-2). Plaintiff received a notice of the breach from Mercyhurst on or about November 8, 2022, which stated that the compromised information included, at least, his name, financial account number, and Social Security number. (Id. at ¶ 45). The notice further encouraged Plaintiff to "remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity." (Id. at ¶ 38). In addition, Mercyhurst offered to provide free credit monitoring protection services for twelve months (Id. at ¶ 39).

After receiving the notice from Mercyhurst, Plaintiff spent, and continues to spend, considerable time and effort monitoring his accounts to protect himself from identity theft, including regularly monitoring his credit report and locking his credit cards. (Id. at ¶¶ 47-48). As

[1] The factual history set forth herein has been gleaned from the allegations of Plaintiff's complaint [ECF No. 1-2], which are accepted as true for purposes of considering Defendant's motion, to the extent such allegations are well-pleaded.

a result, Plaintiff claims that he has suffered "feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach." (Id. at ¶ 48).

II. DISCUSSION

A. Subject Matter Jurisdiction – Article III Standing

Mercyhurst first argues that this action must be dismissed because Plaintiff lacks Article III standing. A motion to dismiss predicated on a lack of standing presents a jurisdictional matter and thus is "properly brought pursuant to Rule 12(b)(1)." Ballentine v. United States, 486 F.3d 806, 810 (3d Cir. 2007).

1. Standard of Review – Fed.R.Civ.P. 12(b)(1)

Two types of challenges to the court's subject matter jurisdiction can be asserted under Rule 12(b)(1) - facial or factual. In re Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 632 (3d Cir. 2017), citing Davis v. Wells Fargo, 824 F.3d 333, 346 (3d Cir. 2016)). "[A] facial attack 'contests the sufficiency of the pleadings, . . . whereas a factual attack concerns the actual failure of a [plaintiff's] claims to comport [factually] with the jurisdictional prerequisites.'" The Constitution Party of Pa. v. Aichele, 757 F.3d 347, 358 (3d Cir. 2014) (internal citations omitted). Here, Mercyhurst is bringing a facial challenge to Plaintiff's standing.

"In reviewing a facial attack, 'the court must only consider the allegations of the complaint and documents referenced therein and attached thereto, in the light most favorable to the plaintiff.'" Id., quoting In re Schering Plough Corp. Intron/Temodar Consumer Class Action, 678 F.3d 235, 243 (3d Cir. 2012) (other citation omitted). Thus, a facial challenge requires the court to apply the same legal standard it would apply in ruling on a motion to dismiss under Rule 12(b)(6). Id., citing In re Schering Plough Corp., 678 F.3d at 243. Consequently, "'[t]o survive a

motion to dismiss [for lack of standing], a complaint must contain sufficient factual matter' that would establish standing if accepted as true." In re Horizon Healthcare Servs., 846 F.3d at 633, quoting Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (citation omitted). At the pleading stage, the plaintiff bears the burden of establishing that he has standing to sue. Reilly v. Ceridian Corp., 664 F.3d 38, 41 (3d Cir. 2011), citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992); Storino v. Borough of Point Pleasant Beach, 322 F.3d 293, 296 (3d Cir. 2003).

In order to have standing, a plaintiff must demonstrate: "(1) that he suffered an injury in fact that is concrete, particularized, and actual or imminent, (2) that the injury was caused by the defendant, and (3) that the injury would likely be redressed by the requested judicial relief." Clemens v. ExecuPharm Inc., 48 F.4th 146, 152 (3d Cir. 2022) citing Thole v. U.S. Bank N.A., 590 U.S. ___, 140 S. Ct. 1615, 1618 (2020).

2. Injury in Fact

Here, Mercyhurst appears to be challenging only the first element of Article III standing— whether Plaintiff suffered an injury in fact. In Spokeo, Inc. v. Robins, 578 U.S. 330 (2016), the Supreme Court provided guidance as to what constitutes a concrete injury - "[a] 'concrete' injury must be 'de facto'; that is, it must actually exist." 578 U.S. at 340 (citations omitted). With regard to the "actual" or imminent" element of the injury in fact test, the Third Circuit has opined: "A harm is 'actual or imminent' rather than 'conjectural or hypothetical' where it is presently or actually occurring or is sufficiently imminent.... [P]laintiffs relying on claims of imminent harm must demonstrate that they face a realistic danger of sustaining a direct injury from the conduct of which they complain." Blunt v. Lower Merion Sch. Dist., 767 F.3d 247, 278 (3d Cir. 2014) (citation omitted). "Allegations of possible future injury do not satisfy

the requirements of Art. III. A threatened injury must be 'certainly impending' to constitute injury in fact." Whitmore v. Arkansas, 495 U.S. 149, 158 (1990) (citation omitted).

Here, Mercyhurst argues that "a mere risk of identity theft that has not actually materialized is not sufficient to constitute a concrete injury necessary to confer Article III standing in the Third Circuit." (ECF No. 15, at p. 6). In making this argument, Plaintiff principally relies on the Third Circuit Court's decision in Reilly v. Ceridian Corp., 664 F.3d 38, 43 (3d Cir. 2011), and its progeny.

Reilly, like the present case, involved a data security breach perpetrated by a hacker who infiltrated the defendant's payroll processing system and "potentially gained access to personal and financial information" belonging to nearly 30,000 people, but it was "not known whether the hacker read, copied, or understood the data." Id. at 40. The Court found the allegations insufficient to establish imminent injury because it could not describe how the plaintiffs would be injured "without beginning [its] explanation with the word "if"; if the hacker read, copied, and understood the hacked information, and if the hacker attempts to use the information, and if he does so successfully, only then will [plaintiffs] have suffered an injury." Id. (emphasis in original). As such, the plaintiffs' allegations relied solely on conjecture: there were no allegations that their personal information had actually been compromised or misused; instead, plaintiffs merely alleged potential, future harm due to the breach. Id. at 42. Thus, the Third Circuit concluded that the plaintiffs lacked standing, holding that, in "data breach cases where no misuse is alleged, … there has been no injury," because any future injuries are "entirely speculative and dependent on the skill and intent of the hacker…." Id. at 45. The Court also noted that allegations of lost time and expenditures incurred by the plaintiffs to monitor their financial information following a data breach are also insufficient to confer Article III standing

"because costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts" are not injuries that are actual or imminent. Id. at 46.

Mercyhurst notes that, as in Reilly, Plaintiff in this case "makes no specific allegations that he suffered any identity theft, or that the unauthorized actor who may have illegally accessed Mercyhurst's network did anything at all with the class members' PII, other than hold it for ransom." (ECF No. 15, at p. 6). Thus, Mercyhurst argues that Plaintiff "has not articulated an injury in fact and only presents speculative future risk of harm as a result of the [Data Breach]," which "alone is not enough to confer standing before this Court…." (ECF No. 15, at p. 5).

In opposition, Plaintiff argues that Mercyhurst's assertion that "a victim of a data breach only has standing if they have been the victim of identity theft… is directly contradicted by the Third Circuit's recent decision in *Clemens v. ExecuPharm, Inc.*, which states unambiguously: 'we did not create a bright line rule precluding standing based on the alleged risk of identity theft or fraud.' 48 F.4th 146, 153 (3d Cir. 2022)" (ECF No. 19, at p. 3). Instead, the Circuit Court in Clemens clarified its prior holding in Reilly, noting that "*Reilly* requires consideration of whether an injury is present versus future, and imminent versus hypothetical." Id. The Third Circuit then "identified a set of non-exhaustive factors" for courts to consider in the context of a data breach to determine whether a plaintiff alleges an "imminent injury" that satisfies the "injury-in-fact" requirement: "1) whether the data breach was intentional; 2) whether the data was misused; and 3) whether the nature of the information accessed through a data breach could subject a plaintiff to a risk of identity theft." Clemens, 48 F.4th 146, 153-54. Weighing these factors, the Clemens Court determined that, based on the facts in that case, the plaintiff's risk of injury was sufficiently imminent to constitute an injury in fact for purposes of standing.

Plaintiff argues that the facts alleged in the present case are more analogous to the facts alleged in Clemens, rather than Reilly, thus leading to the conclusion that Plaintiff has sufficiently alleged an injury in fact to establish standing. To assess this argument, the Court looks to the Third Circuit's own comparison of its two cases in Clemens, to illuminate the factors the Circuit Court found most relevant in distinguishing Clemens from Reilly:

> In *Reilly*, we had occasion to discuss the contours of the injury-in-fact requirement in the data breach context. This time, the alleged injury-in-fact is far more imminent. Whereas *Reilly* involved an *unknown* hacker who *potentially* gained access to sensitive information, 664 F.3d at 42-43; here, a known hacker group named CLOP accessed Clemens's sensitive information. CLOP is a sophisticated ransomware group that is notorious for encrypting companies' internal data and placing in every digital folder a text file called 'ClopReadMe.txt' that contains a message demanding ransom. These attacks are particularly threatening given that, according to a data specialist, there are 'no known decryption tools for CLOP ransomware.'
>
> In this instance, CLOP launched its signature attack against ExecuPharm: it encrypted ExecuPharm's information and held it for ransom. Further, **while the injury to the plaintiffs in *Reilly* depended upon a string of hypotheticals being borne out**, 664 F.3d at 43, **CLOP has already published Clemens's data on the Dark Web, a platform that facilitates criminal activity worldwide**. Clemens has alleged that the Dark Web is 'most widely used as an underground black market where individuals sell illegal products like drugs, weapons, counterfeit money, and sensitive stolen data that can be used to commit identity theft or fraud.'
>
> **Because we can reasonably assume that many of those who visit the Dark Web, and especially those who seek out and access CLOP's posts, do so with nefarious intent, it follows that Clemens faces a substantial risk of identity theft or fraud by virtue of her personal information being made available on underground websites. This set of facts clearly presents a more imminent injury than the ones we deemed to establish only a hypothetical injury in *Reilly*.**

Clemens, 48 F4th. 156-57 (emphasis in bold added; emphasis in italics in original).

Based on the foregoing comparison, the Third Circuit in Clemens concluded that, unlike in Reilly, the plaintiffs had established an imminent injury sufficient to establish standing

because the facts indicated that hackers "*intentionally* gained access to and *misused* the data: [they] launched a sophisticated phishing attack to install malware, encrypted the data, held it for ransom, and published it." Id. at 157 (emphasis in original).

Such is not the case here. Unlike in Clemens, there is no allegation that the information compromised by the Data Breach in the present case was ever published on the Dark Web or otherwise distributed or made available to "nefarious" third parties. Indeed, the facts of the present case more closely mirror those in Reilly, where, as here, it was not known whether the hacker(s) even "read, copied, or understood the data." Reilly, 664 F.3d at 40. See also McGowan v. Core Cashless, LLC, 2024 WL 488318, at *2 (W.D. Feb. 8, 2024) (Finding that, even where plaintiff alleged that the Secret Service had identified payment card numbers for sale on the Dark Web that were likely obtained from a payment processor used by defendant, plaintiff failed to allege the same type of malicious and sophisticated intent that existed in Clemens); In re Am. Fin. Res., Inc. v. Data Breach Litig., 2023 WL 3963804 at *5 (D.N.J. Mar. 29, 2023) ("Although Plaintiffs generally state that "criminals" hacked into AFR's systems with the intent to misuse PII, unlike in Clemens, the intentions and methods of the AFR data breach hacker(s) are entirely unknown").

As in Reilly and its progeny, Plaintiff has failed to plausibly show that his threatened risk of harm from the Data Breach is imminent. As such, the Court finds that Plaintiff has failed to show that he sustained a plausible injury in fact sufficient to establish Article III standing.[2]

2

Because the Court has determined that Plaintiff has failed to plausibly show that he has Article III standing to pursue this action, there is no need for the Court to consider Mercyhurst's motion to dismiss the complaint under Rule 12(b)(6).

B. Remand to State Court

Plaintiff asserts that, in the event the Court determines that it does not have subject matter jurisdiction over this matter due to Plaintiff's lack of Article III standing, the Court must remand this case to the state court from which it was removed. The Court agrees.

As noted at the outset, this case was originally filed in the Court of Common Pleas of Erie County, Pennsylvania, and was subsequently removed to this Court by Defendant. When a federal court determines that it lacks subject matter jurisdiction over a case that has been removed from state court, the plain language of 28 U.S.C. § 14, 500 U.S 47(c)[3] requires that the matter be remanded to the state court from which it was removed. The Third Circuit Court has noted that "[t]he language of this section is mandatory – once the federal court determines that it lacks jurisdiction, it must remand the case back to the appropriate state court." Bromwell v. Michigan Mut. Ins. Co., 155 F.3d 208, 213 (1997), citing International Primate Protection League v. Administrators of Tulane Educ. Fund, 500 U.S. 72, 87 (1991); Maine Assoc. of Independent Neighborhoods v. Comm'r, Maine Dept. of Human Servs., 876 F.2d 1051, 1054 (1st Cir. 1989). See also Johnson v. Patenaude & Felix, A.P.C., 2021 WL 3260064, at *3 (M.D. Pa. July 29, 2021) (citation omitted).

Nonetheless, Mercyhurst counters that remand is not appropriate because Plaintiff failed to move to remand this matter within thirty (30) days after removal to this Court, in accordance with 28 U.S.C. § 1447(c), and is only now "circuitously seek[ing] to shoehorn in a quasi-motion to remand." However, this argument is specious because Section 1447(c) plainly requires remand

---

[3] 28 U.S.C. § 1447(c) provides: "If at any time before final judgment it appears that the district court lacks subject matter jurisdiction, the case **shall** be remanded." (emphasis added).

if the Court determines that it lacks subject matter jurisdiction "at any time before final judgment."

Because the Court has determined that it does not have subject matter jurisdiction over this matter due to Plaintiff's lack of standing, the Court will remand this matter to the state court in accordance with the mandate of 28 U.S.C. § 1447(c).

An appropriate Order follows.